RADIUS를 사용하여 레이어 2 터널 프로토콜 인증 구성

목차

소개

이 문서에서는 RADIUS 서버에서 다운로드한 터널 특성을 사용하여 L2TP(Layer 2 Tunnel Protocol) VPDN(Virtual Private Dialup Network) 시나리오를 구성하는 방법을 설명합니다. 이 예에서는 LAC(L2TP Access Concentrator)가 들어오는 연결을 수신하여 LAC RADIUS 서버에 연결합니다. RADIUS 서버는 사용자의 도메인(예: cisco.com)에 대한 터널 특성을 조회하고 LAC에 터널 특성을 전달합니다. 이러한 특성을 기반으로 LAC는 L2TP 네트워크 서버(LNS)에 대한 터널을 시작합니다. 터널이 설정되면 LNS는 자체 RADIUS 서버를 사용하여 최종 사용자를 인증합니다.

참고: 이 문서에서는 NAS(LAC)가 일반 다이얼 액세스용으로 구성된 것으로 가정합니다. 다이얼을 구성하는 방법에 대한 자세한 내용은 다이얼인 [클라이언트에 대한 기본 AAA RADIUS 구성을 참조하십시오](#).

L2TP 및 VPDN에 대한 자세한 내용은 다음 문서를 참조하십시오.

- VPDN 이해
- 가상 사설 네트워크 구성
- 레이어 2 터널 프로토콜

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 2511 라우터 2개
- Cisco IOS® 소프트웨어 릴리스 12.0(2).T
- Cisco Secure ACS for UNIX, Cisco Secure ACS for Windows 또는 Merit RADIUS

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

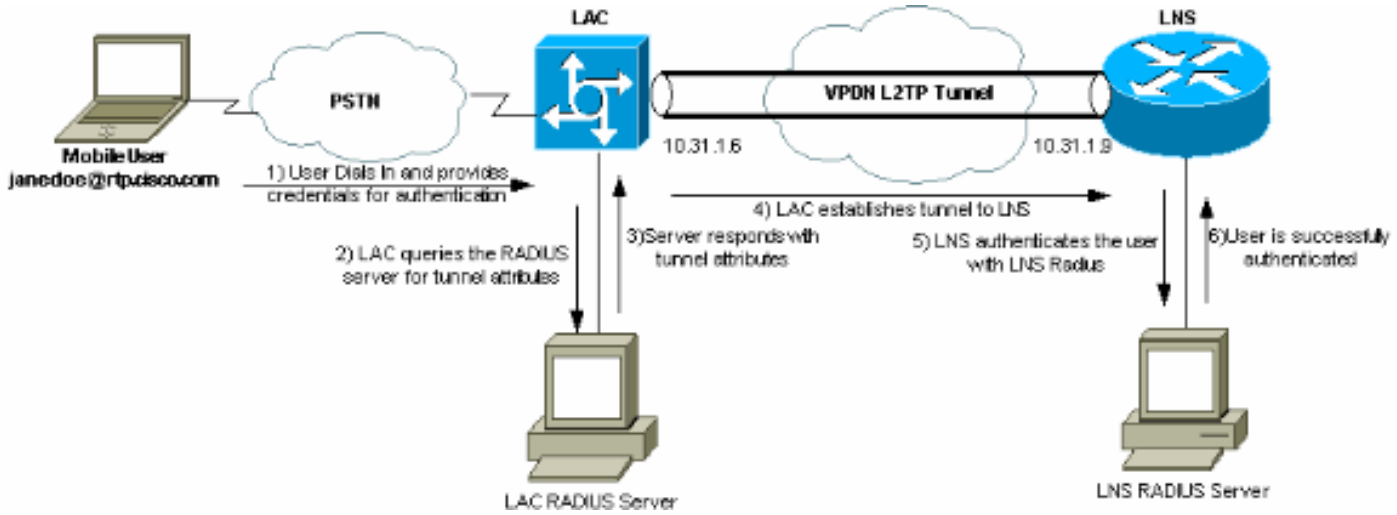
RADIUS 서버 컨피그레이션

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에 사용된 명령에 대한 추가 정보를 보려면 명령 조회 도구(등록된 고객만 해당)를 사용하십시오.

네트워크 다이어그램

이 문서에서는 이 다이어그램에 나와 있는 네트워크 설정을 사용합니다.



LAC RADIUS 컨피그레이션 - UNIX용 Cisco Secure ACS

LAC RADIUS 컨피그레이션에는 사용자 "rtp.cisco.com"(클라이언트에서 사용하는 도메인)이 포함됩니다. 이 사용자의 비밀번호는 cisco여야 합니다.

```
# ./ViewProfile -p 9900 -u rtp.cisco.com
user = rtp.cisco.com{
radius=Cisco {
check_items= {
2="cisco"
}
reply_attributes= {
6=5
9,1="vpdn:tunnel-id=DEFGH"
9,1="vpdn:tunnel-type=l2tp"
9,1="vpdn:ip-addresses=10.31.1.9"
9,1="vpdn:l2tp-tunnel-password=ABCDE"
}
}
}
```

LAC의 RADIUS 컨피그레이션에 대한 자세한 내용은 Layer 2 Tunnel Protocol 내의 LAC에서 사용할 RADIUS Profile for Use(RADIUS 프로파일) 섹션을 참조하십시오.

LNS RADIUS 컨피그레이션 - UNIX용 Cisco Secure ACS

```
# ./ViewProfile -p 9900 -u janedoe@rtp.cisco.com
user = janedoe@rtp.cisco.com{
radius=Cisco {
check_items= {
2="rtp"
}
reply_attributes= {
6=2
7=1
}
```

```
}

}
```

LAC RADIUS 컨피그레이션 - Windows용 Cisco Secure ACS

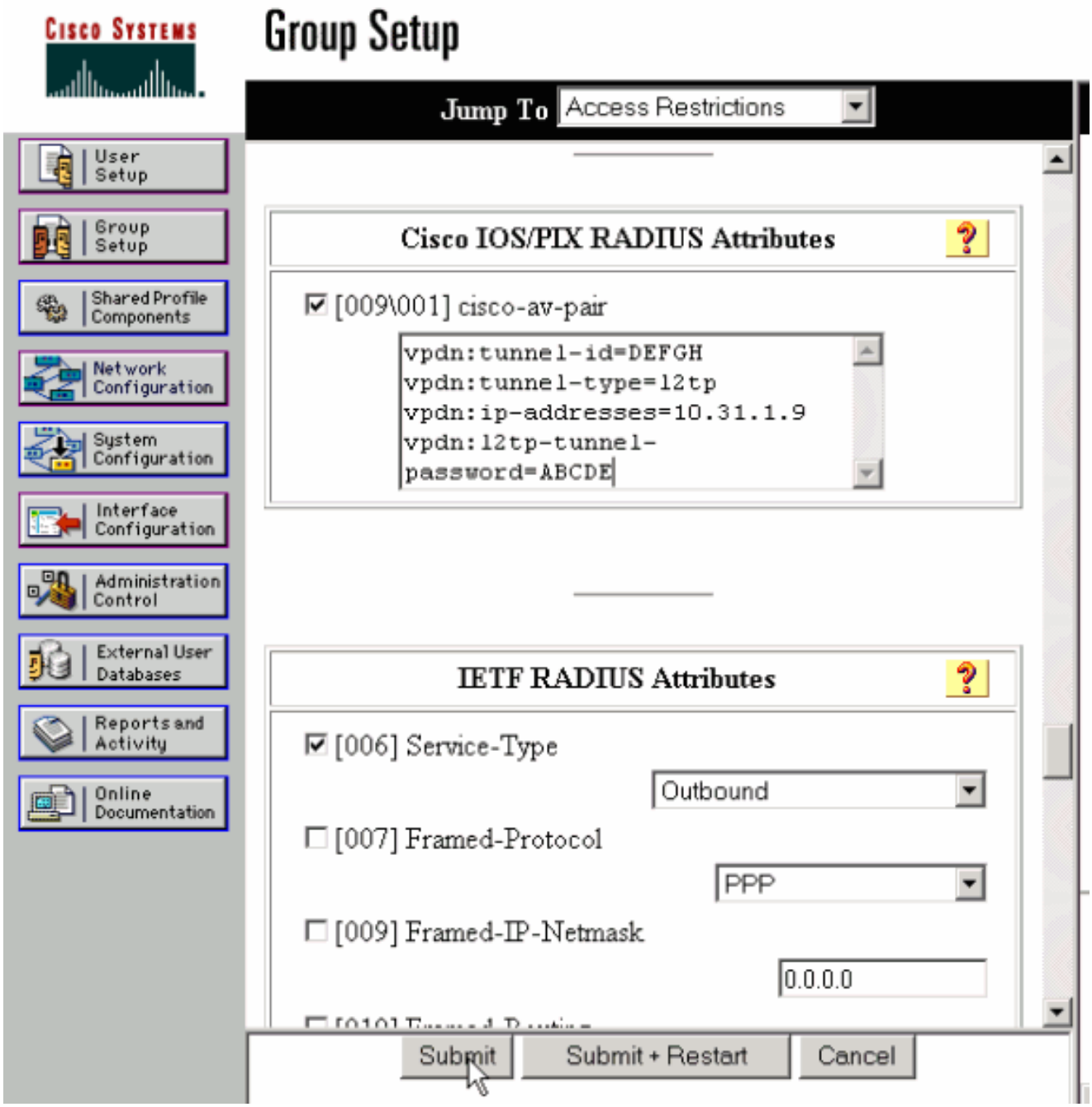
다음 단계를 완료하십시오.

1. Network Configuration(네트워크 컨피그레이션) 영역에서 RADIUS(Cisco IOS/PIX)를 사용하도록 LAC NAS(Network Access Server) 인증을 설정합니다.
2. 일반 및 CHAP에 대해 비밀번호 cisco를 사용하여 사용자 'rtp.cisco.com'을 구성합니다. 터널 특성에 사용되는 사용자 이름입니다.
3. 왼쪽 내비게이션 바에서 Group Setting(그룹 설정) 버튼을 클릭합니다. 사용자가 속한 그룹을 선택하고 설정 편집을 클릭합니다. 아래로 스크롤하여 IETF RADIUS 섹션으로 이동한 다음 Attribute 6 Service-Type을 Outbound로 선택합니다. .

   모든 확인 가능한 옵션이 나타나지 않으면 Interface Configuration(인터페이스 컨피그레이션)으로 이동하여 여러 확인란을 선택하여 그룹 영역에 표시되도록 합니다.
4. 하단의 Cisco IOS/PIX RADIUS 특성 섹션에서 009\001 cisco-av-pair에 대한 확인란을 선택하고 상자에 이를 입력합니다.

   ```
   vpdn:tunnel-id=DEFGH
   vpdn:tunnel-type=l2tp
   vpdn:ip-addresses=10.31.1.9
   vpdn:l2tp-tunnel-password=ABCDE
   ```

   LAC의 RADIUS 컨피그레이션에 대한 자세한 내용은 Layer 2 Tunnel Protocol 내의 LAC에서 사용할 RADIUS Profile for Use(RADIUS 프로파일) 섹션을 참조하십시오.



LNS RADIUS 컨피그레이션 - Windows용 Cisco Secure ACS

다음 단계를 완료하십시오.

1. 사용자 ID janedoe@rtp.cisco.com을 구성하고 일반 및 CHAP에 대한 비밀번호를 입력합니다.
2. 왼쪽 막대에서 Group Setup 버튼을 클릭합니다. 사용자가 속한 그룹을 선택하고 설정 편집을 클릭합니다.
3. IETF(Internet Engineering Task Force) RADIUS Attributes 섹션의 드롭다운 메뉴에서 Service-type (attribute 6) = Framed and Framed-Protocol (attribute 7)=PPP를 선택합니다.

   참고: 선택한 특성 Service-Type 및 Framed-Protocol 옆에 있는 확인란도 클릭해야 합니다.

LAC RADIUS 컨피그레이션 - 장점 RADIUS

참고: Livingston 및 Merit 서버는 공급업체별 av 쌍을 지원하도록 자주 수정해야 합니다.

```
rtp.cisco.com   Password = "cisco"
        Service-Type = Outbound-User,
    cisco-avpair = "vpdn:tunnel-id=DEFGH",
    cisco-avpair = "vpdn:tunnel-type=l2tp",
    cisco-avpair = "vpdn:ip-addresses=10.31.1.9",
    cisco-avpair = "vpdn:l2tp-tunnel-password=ABCDE"
```

LAC의 RADIUS 컨피그레이션에 대한 자세한 내용은 Layer 2 Tunnel Protocol 내의 LAC에서 사용할 RADIUS Profile for Use(RADIUS 프로파일) 섹션을 참조하십시오.

LNS RADIUS 컨피그레이션 - 장점 RADIUS

```
janedoe@rtp.cisco.com   Password = "rtp",
                Service-Type = Framed,
                Framed-Protocol = PPP
```

라우터 컨피그레이션

이 문서에서는 이러한 구성을 사용합니다.

- LAC 라우터 컨피그레이션
- LNS 라우터 컨피그레이션

LAC 라우터 컨피그레이션

```
<#root>

LAC#

show run

Building configuration...

Current configuration:
!
version 12.0
service timestamps debug datetime
service timestamps log uptime
no service password-encryption
!
hostname LAC
!
```

```
!--- AAA commands needed to authenticate the user and obtain !--- VPDN tunnel information.

aaa new-model
aaa authentication login default local
aaa authentication ppp default if-needed radius
aaa authorization network default radius
aaa accounting exec default start-stop radius
aaa accounting network default start-stop radius
enable secret level 7 5 $1$Dj3K$9jkyuJR6fJV2JO./QtOlC1
enable password ww
!
username cse password 0 csecse
username john password 0 doe
ip subnet-zero
no ip domain-lookup
!
jnjOO=tfdfr
vpdn enable
!
!--- VPDN tunnel authorization is based on the domain name !--- (the default is DNIS).

vpdn search-order domain
!
!
!
interface Loopback0
 no ip address
 no ip directed-broadcast
!
interface Ethernet0
 ip address 10.31.1.6 255.255.255.0
 no ip directed-broadcast
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Async1
 ip unnumbered Ethernet0
 no ip directed-broadcast
 ip tcp header-compression passive
 encapsulation ppp
 async mode dedicated
 peer default ip address pool async
 no cdp enable
 ppp authentication chap
!
interface Group-Async1
 physical-layer async
 no ip address
 no ip directed-broadcast
```

```
!
ip local pool default 10.5.5.5 10.5.5.50
ip local pool async 10.7.1.1 10.7.1.5
ip classless
ip route 0.0.0.0 0.0.0.0 10.31.1.1
!

!--- RADIUS server host and key.

radius-server host 171.68.118.101 auth-port 1645 acct-port 1646
radius-server key cisco
!
line con 0
 transport input none
line 1
 session-timeout 20
 exec-timeout 0 0
 password ww
 autoselect during-login
 autoselect ppp
 modem InOut
 transport preferred none
 transport output none
 stopbits 1
 speed 38400
 flowcontrol hardware
line 2 16
 modem InOut
 transport input all
 speed 38400
 flowcontrol hardware
line aux 0
line vty 0 4
 password ww
!
end
```

LNS 라우터 컨피그레이션

<#root>

```
LNS#

show run

Building configuration...

Current configuration:
!
! Last configuration change at 12:17:54 UTC Sun Feb 7 1999
!==m6knr5yui6yt6egv2wr25nfd1rsion 12.0=4rservice exec-callback
service timestamps debug datetime
service timestamps log uptime
no service password-encryption
!
hostname LNS
!
aaa new-model
```

```
aaa authentication login default local
aaa authentication ppp default radius local
aaa authorization network default radius local
aaa accounting exec default start-stop radius
aaa accounting network default start-stop radius
enable secret 5 $1$pnYM$B.FveZjZpgA3C9ZPq/cma/
enable password ww
!
username john password 0 doe

!--- User the_LNS is used to authenticate the tunnel. !--- The password used here must match the vpdn:


username the_LNS password 0 ABCDE

ip subnet-zero
!

!--- Enable VPDN on the LNS.


vpdn enable

!

!--- VPDN group for connection from the LAC.


vpdn-group 1


!--- This command specifies that the router uses !--- virtual-template 1 for tunnel-id DEFGH (which ma


 accept dialin l2tp virtual-template 1 remote DEFGH


!--- The username used to authenticate this tunnel !--- is the_LNS (configured above).


 local name the_LNS

!
interface Ethernet0
 ip address 10.31.1.9 255.255.255.0
 no ip directed-broadcast
!

!--- Virtual-template that is used for the incoming connection.


interface Virtual-Template1

 ip unnumbered Ethernet0
 no ip directed-broadcast
 peer default ip address pool default
 ppp authentication chap
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 no fair-queue
!
```

```
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Async1
 ip unnumbered Ethernet0
 no ip directed-broadcast
 encapsulation ppp
 async mode interactive
 peer default ip address pool async
 ppp authentication chap
!
ip local pool default 10.6.1.1 10.6.1.5
ip local pool async 10.8.100.100 10.8.100.110
ip classless
ip route 0.0.0.0 0.0.0.0 10.31.1.1
!

!--- RADIUS server host and key information.

radius-server host 171.68.120.194 auth-port 1645 acct-port 1646
radius-server key cisco
!
line con 0
 transport input none
line 1
 session-timeout 20
 exec-timeout 5 0
 password ww
 autoselect during-login
 autoselect ppp
 modem InOut
 transport input all
 escape-character BREAK
 stopbits 1
 speed 38400
 flowcontrol hardware
line 2 8
line aux 0
line vty 0 4
 password ww
!
end
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 show 명령은 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 show 명령 출력의 분석 결과를 볼 수 있습니다.

- show vpdn tunnel - 모든 활성 레이어 2 포워딩 및 L2TP 터널에 대한 정보를 요약 스타일 형식으로 표시합니다.
- show caller ip - 제공한 IP 주소에 대한 발신자 정보의 요약을 표시합니다.

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

트러블슈팅 명령

참고: debug 명령을 실행하기 전에 Debug 명령에 대한 중요 정보를 참조하십시오.

- debug aaa authentication(aaa 인증 디버그) - AAA/TACACS+ 인증에 대한 정보를 표시합니다.
- debug aaa authorization(aaa 권한 부여 디버그) - AAA/TACACS+ 권한 부여에 대한 정보를 표시합니다.
- debug aaa accounting(aaa 어카운팅 디버그) - 어카운트가 발생할 때 어카운트에 대한 정보를 표시합니다. 이 명령으로 표시되는 정보는 서버에 어카운팅 정보를 전송하는 데 사용되는 어카운팅 프로토콜과 관련이 없습니다.
- debug radius - RADIUS와 관련된 자세한 디버깅 정보를 표시합니다.
- debug vtemplate - 가상 액세스 인터페이스가 가상 템플릿에서 복제되는 시점부터 호출이 종료될 때 가상 액세스 인터페이스가 종료되는 시점까지의 가상 액세스 인터페이스에 대한 복제 정보를 표시합니다.
- debug vpdn error(디버그 vpdn 오류) - PPP 터널이 설정되지 않도록 하는 오류 또는 설정된 터널이 닫히도록 하는 오류를 표시합니다.
- debug vpdn events(vpdn 이벤트 디버그) - 정상적인 PPP 터널 설정 또는 종료의 일부인 이벤트에 대한 메시지를 표시합니다.
- debug vpdn l2x-errors - 레이어 2 설정을 방해하거나 정상적인 작동을 방해하는 레이어 2 프로토콜 오류를 표시합니다.
- debug vpdn l2x-events - 레이어 2에 대한 정상적인 PPP 터널 설정 또는 종료의 일부인 이벤트에 대한 메시지를 표시합니다.
- debug vpdn l2tp-sequencing - L2TP에 대한 메시지를 표시합니다.

디버그 출력

L2TP 디버깅에 대한 자세한 내용은 L2TP 터널 설정 및 해제를 참조하십시오.

LAC 라우터에서 올바른 디버그

<#root>

LAC#

show debug

```
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on
  AAA Accounting debugging is on
VPN:
  L2X protocol events debugging is on
  L2X protocol errors debugging is on
  VPDN events debugging is on
  VPDN errors debugging is on
  L2TP data sequencing debugging is on
VTEMPLATE:
  Virtual Template debugging is on
Radius protocol debugging is on
LAC#
Feb  7 12:22:16: As1 AAA/AUTHOR/FSM: (0):
    LCP succeeds trivially
2d18h: %LINK-3-UPDOWN: Interface Async1,
    changed state to up
Feb  7 12:22:17: As1 VPDN: Looking for tunnel
    -- rtp.cisco.com --
Feb  7 12:22:17: AAA: parse name=Async1 idb
    type=10 tty=1
Feb  7 12:22:17: AAA: name=Async1 flags=0x11
    type=4 shelf=0 slot=0
    adapter=0 port=1 channel=0
Feb  7 12:22:17: AAA/AUTHEN: create_user (0x25BA84)
    user='rtp.cisco.com' ruser='' port='Async1' rem_addr=''
    authen_type=NONE service=LOGIN priv=0
Feb  7 12:22:17: AAA/AUTHOR/VPDN (6239469):
    Port='Async1' list='default' service=NET
Feb  7 12:22:17: AAA/AUTHOR/VPDN:  (6239469)
    user='rtp.cisco.com'
Feb  7 12:22:17: AAA/AUTHOR/VPDN:  (6239469)
    send AV service=ppp
Feb  7 12:22:17: AAA/AUTHOR/VPDN:  (6239469)
    send AV protocol=vpdn
Feb  7 12:22:17: AAA/AUTHOR/VPDN (6239469)
    found list "default"
Feb  7 12:22:17: AAA/AUTHOR/VPDN:  (6239469) Method=RADIUS
Feb  7 12:22:17: RADIUS: authenticating to get author data
Feb  7 12:22:17: RADIUS: ustruct sharecount=2
Feb  7 12:22:17: RADIUS: Initial Transmit Async1 id 66
    171.68.118.101:1645, Access-Request, len 77
Feb  7 12:22:17:         Attribute 4 6 0A1F0106
Feb  7 12:22:17:         Attribute 5 6 00000001
Feb  7 12:22:17:         Attribute 61 6 00000000
Feb  7 12:22:17:         Attribute 1 15 7274702E
Feb  7 12:22:17:         Attribute 2 18 6AB5A2B0
Feb  7 12:22:17:         Attribute 6 6 00000005
Feb  7 12:22:17: RADIUS: Received from id 66
    171.68.118.101:1645, Access-Accept, len 158
Feb  7 12:22:17:         Attribute 6 6 00000005
Feb  7 12:22:17:         Attribute 26 28 0000000901167670
Feb  7 12:22:17:         Attribute 26 29 0000000901177670
Feb  7 12:22:17:         Attribute 26 36 000000009011E7670
Feb  7 12:22:17:         Attribute 26 39 0000000901217670
Feb  7 12:22:17: RADIUS: saved authorization data for user
    25BA84 at 24C488
```

!--- RADIUS server supplies the VPDN tunnel attributes.

```
Feb  7 12:22:17: RADIUS: cisco AVPair
    "vpdn:tunnel-id=DEFGH"
Feb  7 12:22:17: RADIUS: cisco AVPair
    "vpdn:tunnel-type=l2tp"
Feb  7 12:22:17: RADIUS: cisco AVPair
    "vpdn:ip-addresses=10.31.1.9,"
Feb  7 12:22:17: RADIUS: cisco AVPair
    "vpdn:l2tp-tunnel-password=ABCDE"

Feb  7 12:22:17: AAA/AUTHOR (6239469): Post
    authorization status = PASS_ADD
Feb  7 12:22:17: AAA/AUTHOR/VPDN: Processing
    AV service=ppp
Feb  7 12:22:17: AAA/AUTHOR/VPDN: Processing
    AV protocol=vpdn
Feb  7 12:22:17: AAA/AUTHOR/VPDN: Processing
    AV tunnel-id=DEFGH
Feb  7 12:22:17: AAA/AUTHOR/VPDN: Processing
    AV tunnel-type=l2tp
Feb  7 12:22:17: AAA/AUTHOR/VPDN: Processing AV
    ip-addresses=10.31.1.9,
Feb  7 12:22:17: AAA/AUTHOR/VPDN: Processing AV
    l2tp-tunnel-password=ABCDE
Feb  7 12:22:17: As1 VPDN: Get tunnel info for
    rtp.cisco.com with LAC DEFGH, IP 10.31.1.9
Feb  7 12:22:17: AAA/AUTHEN: free_user (0x25BA84)
    user='rtp.cisco.com' ruser='' port='Async1' rem_addr=''
    authen_type=NONE service=LOGIN priv=0

Feb  7 12:22:17: As1 VPDN: Forward to address 10.31.1.9

Feb  7 12:22:17: As1 VPDN: Forwarding...
Feb  7 12:22:17: AAA: parse name=Async1 idb
    type=10 tty=1
Feb  7 12:22:17: AAA: name=Async1 flags=0x11 type=4
    shelf=0 slot=0 adapter=0 port=1 channel=0
Feb  7 12:22:17: AAA/AUTHEN: create_user (0xB7918)
    user='janedoe@rtp.cisco.com' ruser='' port='Async1'
    rem_addr='async' authen_type=CHAP service=PPP priv=1
Feb  7 12:22:17: As1 VPDN: Bind interface direction=1
Feb  7 12:22:17: Tnl/Cl 51/1 L2TP: Session FS enabled
Feb  7 12:22:17: Tnl/Cl 51/1 L2TP: Session state change
    from idle to wait-for-tunnel
Feb  7 12:22:17: As1 51/1 L2TP: Create session
Feb  7 12:22:17: Tnl 51 L2TP: SM State idle
Feb  7 12:22:17: Tnl 51 L2TP: O SCCRQ
Feb  7 12:22:17: Tnl 51 L2TP: Tunnel state change
    from idle to wait-ctl-reply
Feb  7 12:22:17: Tnl 51 L2TP: SM State wait-ctl-reply

Feb  7 12:22:17: As1 VPDN: janedoe@rtp.cisco.com
    is forwarded

Feb  7 12:22:17: Tnl 51 L2TP: I SCCRP from the_LNS

!--- Tunnel authentication is successful.


Feb  7 12:22:17: Tnl 51 L2TP: Got a challenge from remote
    peer, the_LNS
Feb  7 12:22:17: Tnl 51 L2TP: Got a response from remote
    peer, the_LNS
Feb  7 12:22:17: Tnl 51 L2TP: Tunnel Authentication
    success
```

```
Feb  7 12:22:17: Tnl 51 L2TP: Tunnel state change from
    wait-ctl-reply to established
Feb  7 12:22:17: Tnl 51 L2TP: O SCCCN  to the_LNS tnlid 38
Feb  7 12:22:17: Tnl 51 L2TP: SM State established
Feb  7 12:22:17: As1 51/1 L2TP: O ICRQ to the_LNS 38/O
Feb  7 12:22:17: As1 51/1 L2TP: Session state change from
    wait-for-tunnel to wait-reply
Feb  7 12:22:17: As1 51/1 L2TP: O ICCN to the_LNS 38/1
Feb  7 12:22:17: As1 51/1 L2TP: Session state change from
    wait-reply to established
2d18h: %LINEPROTO-5-UPDOWN: Line protocol on Interface
    Async1, changed state to up
LAC#
```

LNS 라우터에서 디버깅하기 좋음

<#root>

```
LNS#

show debug

General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on
  AAA Accounting debugging is on
VPN:
  L2X protocol events debugging is on
  L2X protocol errors debugging is on
  VPDN events debugging is on
  VPDN errors debugging is on
  L2TP data sequencing debugging is on
VTEMPLATE:
  Virtual Template debugging is on
Radius protocol debugging is on
LNS#
Feb  7 12:22:16: L2TP: I SCCRQ from DEFGH tnl 51


Feb  7 12:22:16: Tnl 38 L2TP: New tunnel created for
    remote DEFGH, address 10.31.1.6

Feb  7 12:22:16: Tnl 38 L2TP: Got a challenge in SCCRQ,
    DEFGH
Feb  7 12:22:16: Tnl 38 L2TP: O SCCRP  to DEFGH tnlid 51
Feb  7 12:22:16: Tnl 38 L2TP: Tunnel state change from
    idle to wait-ctl-reply
Feb  7 12:22:16: Tnl 38 L2TP: I SCCCN from DEFGH tnl 51
Feb  7 12:22:16: Tnl 38 L2TP: Got a Challenge Response
    in SCCCN from DEFGH
Feb  7 12:22:16: Tnl 38 L2TP: Tunnel Authentication
    success
Feb  7 12:22:16: Tnl 38 L2TP: Tunnel state change from
    wait-ctl-reply to established
Feb  7 12:22:16: Tnl 38 L2TP: SM State established
Feb  7 12:22:17: Tnl 38 L2TP: I ICRQ from DEFGH tnl 51
Feb  7 12:22:17: Tnl/Cl 38/1 L2TP: Session FS enabled
Feb  7 12:22:17: Tnl/Cl 38/1 L2TP: Session state change
    from idle to wait-for-tunnel
```

```
Feb  7 12:22:17: Tnl/Cl 38/1 L2TP: New session created
Feb  7 12:22:17: Tnl/Cl 38/1 L2TP: O ICRP to DEFGH 51/1
Feb  7 12:22:17: Tnl/Cl 38/1 L2TP: Session state change
    from wait-for-tunnel to wait-connect
Feb  7 12:22:17: Tnl/Cl 38/1 L2TP: I ICCN from DEFGH tnl
    51, cl 1
Feb  7 12:22:17: Tnl/Cl 38/1 L2TP: Session state change
    from wait-connect to established
Feb  7 12:22:17: Vi1 VTEMPLATE: Reuse Vi1, recycle
    queue size 0
Feb  7 12:22:17: Vi1 VTEMPLATE: Hardware address
    00e0.1e68.942c

!--- Use Virtual-template 1 for this user.


Feb  7 12:22:17: Vi1 VPDN: Virtual interface created for
    janedoe@rtp.cisco.com
Feb  7 12:22:17: Vi1 VPDN: Set to Async interface
Feb  7 12:22:17: Vi1 VPDN: Clone from Vtemplate 1
    filterPPP=0 blocking

Feb  7 12:22:17: Vi1 VTEMPLATE: Has a new cloneblk vtemplate,
    now it has vtemplate
Feb  7 12:22:17: Vi1 VTEMPLATE: ************* CLONE
    VACCESS1 *****************
Feb  7 12:22:17: Vi1 VTEMPLATE: Clone from
    Virtual-Template1
interface Virtual-Access1
default ip address
no ip address
encap ppp
ip unnum eth 0
no ip directed-broadcast
peer default ip address pool default
ppp authen chap
end

Feb  7 12:22:18: janedoe@rtp.cisco.com 38/1 L2TP: Session
    with no hwidb
02:23:59: %LINK-3-UPDOWN: Interface Virtual-Access1,
    changed state to up
Feb  7 12:22:19: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds
    trivially
Feb  7 12:22:19: Vi1 VPDN: Bind interface direction=2
Feb  7 12:22:19: Vi1 VPDN: PPP LCP accepted rcv CONFACK
Feb  7 12:22:19: Vi1 VPDN: PPP LCP accepted sent CONFACK
Feb  7 12:22:19: Vi1 L2X: Discarding packet because of
    no mid/session
Feb  7 12:22:19: AAA: parse name=Virtual-Access1 idb
    type=21 tty=-1
Feb  7 12:22:19: AAA: name=Virtual-Access1 flags=0x11
    type=5 shelf=0 slot=0 adapter=0 port=1 channel=0
Feb  7 12:22:19: AAA/AUTHEN: create_user (0x2462A0)
    user='janedoe@rtp.cisco.com' ruser='' port='Virtual-Access1'
    rem_addr='' authen_type=CHAP service=PPP priv=1
Feb  7 12:22:19: AAA/AUTHEN/START (2229277178):
    port='Virtual-Access1' list='' action=LOGIN
    service=PPP
Feb  7 12:22:19: AAA/AUTHEN/START (2229277178):
    using "default" list
Feb  7 12:22:19: AAA/AUTHEN/START (2229277178):
    Method=RADIUS
```

```
Feb  7 12:22:19: RADIUS: ustruct sharecount=1
Feb  7 12:22:19: RADIUS: Initial Transmit Virtual-Access1
    id 78 171.68.120.194:1645, Access-Request, len 92
Feb  7 12:22:19:         Attribute 4 6 0A1F0109
Feb  7 12:22:19:         Attribute 5 6 00000001
Feb  7 12:22:19:         Attribute 61 6 00000005
Feb  7 12:22:19:         Attribute 1 23 6464756E
Feb  7 12:22:19:         Attribute 3 19 34A66389
Feb  7 12:22:19:         Attribute 6 6 00000002
Feb  7 12:22:19:         Attribute 7 6 00000001
Feb  7 12:22:19: RADIUS: Received from id 78
    171.68.120.194:1645, Access-Accept, len 32
Feb  7 12:22:19:         Attribute 6 6 00000002
Feb  7 12:22:19:         Attribute 7 6 00000001
Feb  7 12:22:19: AAA/AUTHEN (2229277178): status = PASS
Feb  7 12:22:19: Vi1 AAA/AUTHOR/LCP: Authorize LCP
Feb  7 12:22:19: AAA/AUTHOR/LCP Vi1 (1756915964):
    Port='Virtual-Access1' list='' service=NET
Feb  7 12:22:19: AAA/AUTHOR/LCP: Vi1 (1756915964)
    user='janedoe@rtp.cisco.com'
Feb  7 12:22:19: AAA/AUTHOR/LCP: Vi1 (1756915964)
    send AV service=ppp
Feb  7 12:22:19: AAA/AUTHOR/LCP: Vi1 (1756915964)
    send AV protocol=lcp
Feb  7 12:22:19: AAA/AUTHOR/LCP (1756915964) found
    list "default"
Feb  7 12:22:19: AAA/AUTHOR/LCP: Vi1 (1756915964)
    Method=RADIUS
Feb  7 12:22:19: AAA/AUTHOR (1756915964): Post
    authorization status = PASS_REPL
Feb  7 12:22:19: Vi1 AAA/AUTHOR/LCP: Processing
    AV service=ppp
Feb  7 12:22:19: AAA/ACCT/NET/START User
    janedoe@rtp.cisco.com, Port Virtual-Access1, List ""
Feb  7 12:22:19: AAA/ACCT/NET: Found list "default"
Feb  7 12:22:19: Vi1 AAA/AUTHOR/FSM: (0): Can we
    start IPCP?
Feb  7 12:22:19: AAA/AUTHOR/FSM Vi1 (1311872588):
    Port='Virtual-Access1' list='' service=NET
Feb  7 12:22:19: AAA/AUTHOR/FSM: Vi1 (1311872588)
    user='janedoe@rtp.cisco.com'
Feb  7 12:22:19: AAA/AUTHOR/FSM: Vi1 (1311872588)
    send AV service=ppp
Feb  7 12:22:19: AAA/AUTHOR/FSM: Vi1 (1311872588)
    send AV protocol=ip
Feb  7 12:22:19: AAA/AUTHOR/FSM (1311872588)
    found list "default"
Feb  7 12:22:19: AAA/AUTHOR/FSM: Vi1 (1311872588)
    Method=RADIUS
Feb  7 12:22:19: AAA/AUTHOR (1311872588): Post
    authorization status = PASS_REPL
Feb  7 12:22:19: Vi1 AAA/AUTHOR/FSM: We can start
    IPCP
Feb  7 12:22:19: RADIUS: ustruct sharecount=2
Feb  7 12:22:19: RADIUS: Initial Transmit Virtual-Access1
    id 79 171.68.120.194:1646, Accounting-Request, len 101
Feb  7 12:22:19:         Attribute 4 6 0A1F0109
Feb  7 12:22:19:         Attribute 5 6 00000001
Feb  7 12:22:19:         Attribute 61 6 00000005
Feb  7 12:22:19:         Attribute 1 23 6464756E
Feb  7 12:22:19:         Attribute 40 6 00000001
Feb  7 12:22:19:         Attribute 45 6 00000001
```

```
Feb  7 12:22:19:         Attribute 6 6 00000002
Feb  7 12:22:19:         Attribute 44 10 30303030
Feb  7 12:22:19:         Attribute 7 6 00000001
Feb  7 12:22:19:         Attribute 41 6 00000000
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Start.  Her
    address 0.0.0.0, we want 0.0.0.0
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Processing
    AV service=ppp
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Authorization
    succeeded
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Done.  Her
    address 0.0.0.0, we want 0.0.0.0
Feb  7 12:22:19: RADIUS: Received from id 79
    171.68.120.194:1646, Accounting-response,
    len 20
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Start.
    Her address 0.0.0.0, we want 10.6.1.1
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Processing
    AV service=ppp
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Authorization
    succeeded
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Done.
    Her address 0.0.0.0, we want 10.6.1.1
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Start.
    Her address 10.6.1.1, we want 10.6.1.1
Feb  7 12:22:19: AAA/AUTHOR/IPCP Vi1 (2909132255):
    Port='Virtual-Access1' list='' service=NET
Feb  7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255)
    user='janedoe@rtp.cisco.com'
Feb  7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255)
    send AV service=ppp
Feb  7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255)
    send AV protocol=ip
Feb  7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255)
    send AV addr*10.6.1.1
Feb  7 12:22:19: AAA/AUTHOR/IPCP (2909132255)
    found list "default"
Feb  7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255)
    Method=RADIUS
Feb  7 12:22:19: AAA/AUTHOR (2909132255): Post
    authorization status = PASS_REPL
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Reject
    10.6.1.1, using 10.6.1.1
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Processing
    AV service=ppp
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Processing
    AV addr*10.6.1.1
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Authorization
    succeeded
Feb  7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Done.
    Her address 10.6.1.1, we want 10.6.1.1
02:24:00: %LINEPROTO-5-UPDOWN: Line protocol on
    Interface Virtual-Access1, changed state to up
LNS#
```

What Can Go Wrong - LAC의 불량 디버그

```
LAC#
```

show debug

```
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on
  AAA Accounting debugging is on
VPN:
  L2X protocol events debugging is on
  L2X protocol errors debugging is on
  VPDN events debugging is on
  VPDN errors debugging is on
  L2TP data sequencing debugging is on
VTEMPLATE:
  Virtual Template debugging is on
Radius protocol debugging is on
```

사용자가 janedoe@sj.cisco.com으로 들어오지만(janedoe@rtp.cisco.com 대신) LAC RADIUS 서버가 이 도메인을 인식하지 못합니다.

<#root>

```
Feb  7 13:26:48: RADIUS: Received from id 86
    171.68.118.101:1645, Access-Reject, len 46
Feb  7 13:26:48:         Attribute 18 26 41757468
Feb  7 13:26:48: RADIUS: failed to get
    authorization data: authen status = 2
%VPDN-6-AUTHORFAIL: L2F NAS LAC, AAA authorization
    failure for As1 user janedoe@sj.cisco.com
```

이러한 디버깅은 터널 정보가 수신되지만 터널의 다른 끝에 대해 유효하지 않은 IP 주소가 있는 상황을 보여줍니다. 사용자가 세션 설정을 시도하지만 연결할 수 없습니다.

<#root>

```
Feb  7 13:32:45: As1 VPDN: Forward to
    address 1.1.1.1
Feb  7 13:32:45: As1 VPDN: Forwarding...
Feb  7 13:32:45: Tnl 56 L2TP: Tunnel state
    change from idle to wait-ctl-reply
Feb  7 13:32:46: As1 56/1 L2TP: Discarding data
    packet because tunnel is not open
```

이러한 디버깅은 터널 암호가 일치하지 않는 상황을 보여 줍니다. LNS에서 "username the_LNS password ABCDE"가 "username the_LNS password garbage"로 변경되어 터널 인증이 시도될 때 실패합니다.

<#root>

```
Feb  7 13:39:35: Tnl 59 L2TP: Tunnel Authentication
    fails for the_LNS
Feb  7 13:39:35: Tnl 59 L2TP: Expected
    E530DA13B826685C678589250C0BF525
Feb  7 13:39:35: Tnl 59 L2TP: Got
   E09D90E8A91CF1014C91D56F65BDD052
Feb  7 13:39:35: Tnl 59 L2TP: O StopCCN
    to the_LNS tnlid 44
Feb  7 13:39:35: Tnl 59 L2TP: Tunnel state
    change from wait-ctl-reply to shutting-down
Feb  7 13:39:35: Tnl 59 L2TP: Shutdown tunnel
```

What Can Go Wrong - LNS에서 불량 디버그

<#root>

```
LNS#

show debug

General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on
  AAA Accounting debugging is on
VPN:
  L2X protocol events debugging is on
  L2X protocol errors debugging is on
  VPDN events debugging is on
  VPDN errors debugging is on
  L2TP data sequencing debugging is on
VTEMPLATE:
  Virtual Template debugging is on
Radius protocol debugging is on
LNS#
```

이 예에서는 "전화 걸기 l2tp virtual-template 1 remote DEFGH 허용"이 "전화 걸기 l2tp virtual-template 1 remote junk 허용"으로 변경됩니다. LNS에서 터널 DEFGH를 더 이상 찾을 수 없습니다(대신 "정크").

<#root>

```
Feb  7 13:45:32: L2TP: I SCCRQ from
    DEFGH tnl 62
Feb  7 13:45:32: L2X: Never heard of
    DEFGH
Feb  7 13:45:32: L2TP: Could not find info
    block for DEFGH
```

LNS 어카운팅 레코드

```
10.31.1.9 janedoe@rtp.cisco.com 1 - start
    server=rtp-cherry time=09:23:53
    date=02/ 6/1999 task_id=0000001C
Sat Feb 6 12:23:53 1999
        Client-Id = 10.31.1.9
        Client-Port-Id = 1
        NAS-Port-Type = Virtual
        User-Name = "janedoe@rtp.cisco.com"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        User-Service-Type = Framed-User
        Acct-Session-Id = "0000001C"
        Framed-Protocol = PPP
        Acct-Delay-Time = 0


10.31.1.9 janedoe@rtp.cisco.com 1 - stop
    server=rtp-cherry time=09:24:46
    date=02/ 6/1999 task_id=0000001C
Sat Feb  6 12:24:46 1999
        Client-Id = 10.31.1.9
        Client-Port-Id = 1
        NAS-Port-Type = Virtual
        User-Name = "janedoe@rtp.cisco.com"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        User-Service-Type = Framed-User
        Acct-Session-Id = "0000001C"
        Framed-Protocol = PPP
        Framed-Address = 10.6.1.1
        Acct-Terminate-Cause = Lost-Carrier
        Acct-Input-Octets = 678
        Acct-Output-Octets = 176
        Acct-Input-Packets = 17
        Acct-Output-Packets = 10
        Acct-Session-Time = 53
        Acct-Delay-Time = 0
```

관련 정보

- L2TP를 사용하여 VPDN 다이얼 인 액세스
- 레이어 2 터널 프로토콜
- RADIUS 지원 페이지
- Windows용 Cisco Secure ACS 지원 페이지
- UNIX용 Cisco Secure ACS 지원 페이지
- RFC(설명 요청)
- Technical Support - Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.